Chapter 4 Applications of the Euclidean Algorithms

- Modular arithmetic
- Modular inverses
- Linear Diophantine equations
- Continued fractions

4.1 Modular arithmetic

We take a single-precision prime p and check whether $a \cdot b$ and c are congruent modular p:

$$a \cdot b \equiv c \bmod p \Longleftrightarrow p | (a \cdot b - c)$$

We also can test equalities for polynomials $f \cdot g = h$ by substituting a random value.

Definition 1. *Computing with remainders of arithmetic expressions modular some nonzero integer is called modular arithmetic.*

The basic rule for computing with congruences is

$$a \equiv b \bmod m \Longrightarrow a \cdot c \equiv b \cdot c \bmod m$$

For example

$$e = 20 \cdot (-89) + 32 \equiv 6 \cdot 2 + 4 \equiv 12 + 4 \equiv 5 + 4 \equiv 9 \equiv 2 \bmod 7$$

We have to be careful about cancellation and division.

$$0 \cdot 2 \equiv 2 \cdot 2 \equiv 0 \text{ mod } 4, \text{ but } 0 \not\equiv 2 \text{ mod } 4$$

We can also perform modular arithmetic with polynomials over a ring R. Here the simplest nontrivial modulus is a linear polynomial $x - u$ with $u \in R$:

$$f \text{ rem } (x-u) = f(u) \text{ and } f \equiv f(u) \text{ mod } (x-u)$$

If the polynomial modulus is not linear, then the remainder of a polynomial f on division by $m(x)$ is a unique polynomial of degree less than $\deg m(x)$. For $f = x^3$, we have

$$x^3 \equiv 2x + 1 \text{ mod } x^2 - x - 1$$

Definition 2. *If R is a ring(say $R = \mathbb{Z}$ or $R = F[x]$) and $m \in R$, then $< m >= mR = \{mr : r \in R\}$ the multiples of m is the ideal generated by m and the residue class ring*

$$R/mR = R/ < m >= \{f \text{ mod } m : f \in R\}$$

consists of all residue classes

$$f \text{ mod } m = \{f + mr : r \in R\} \text{ for } f \in R$$

The residue class f mod m is represented by its smallest nonnegative element in the case $R = \mathbb{Z}$ and by its unique polynomial of least degree in the case $R = F[x]$.

$$\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

4.2 Modular inverses via Euclid

Theorem 1. *Let* R *be a Euclidean domain,* $a, m \in R$*, and* $S = R/mR$*. Then* a *mod* $m \in S$ *is unit if and only if* $\gcd(a, m) = 1$*. In this case, the modular inverse of* a *mod* m *can be computed by means of the Extended Euclidean Algorithm.*

$$a \text{ is invertible modulo } m \Leftrightarrow \exists s \in R, sa \equiv 1 \bmod m$$
$$\Longleftrightarrow \exists s, t \in R: \; sa + tm = 1 \Longleftrightarrow \gcd(a, m) = 1.$$

For example $R = \mathbb{Z}, m = 29, a = 12$. Then $\gcd(a, m) = 1$ and EEA computes

$$5 \cdot 29 + (-12) \cdot 12 = 1.$$

Thus

$$(-12) \cdot 12 \equiv 17 \cdot 12 \equiv 1 \text{ mod } 29,$$

hence 17 is the inverse of 12 modulo 29.

Corollary 1. *If* $S = \mathbb{Z}_p$ *for a prime* $p \in \mathbb{N}$ *or* $S = F[x]/ < f >$ *for a field* F *and an irreducible polynomial* $f \in F[x]$*, then any element of* $S/ \{0\}$ *is a unit, so that* S *is a field.*

We will use $\mathbb{F}_p$ for the finite field $\mathbb{Z}_p$. More generally, if $f \in Z_p[x] = \mathbb{F}_p[x]$ is an irreducible polynomial of degree n, then $\mathbb{F}_p[x]/ < f >$ is a finite field with $q = p^n$ elements, denoted by $\mathbb{F}_q$.

For example, $R = \mathbb{F}_5[x], f = x^3 - x + 2$. f is irreducible in $\mathbb{F}_5$. Thus $\mathbb{F}_{5^3} = \mathbb{F}_{125} = \mathbb{F}_5[x]/ < f >$ is a field.

Lemma 1. *Let F be a field, $f \in F[x]$ a monic nonconstant irreducible polynomial,and $K = F[x]/ < f >$. Then K is an extension field of f, and $f(\alpha) = 0$ for $\alpha = (x \text{ mod } f) \in K$.*

Corollary 2. *Let F be a field,and $f \in F[x]$ of degree $n \in \mathbb{N}$. One arithmetic operation in $F[x]/ < f >$, that is, addition, multiplication, or division by an invertible element, can be done using $O(n^2)$ arithmetic operations in F. More precisely, we have at most $4n^2 + O(n)$ operations for a multiplication modulo f and at most $\frac{13}{2}n^2 + O(n)$ operations for an inversion modulo f.*

4.3 Modular inverses via Fermat

Theorem 2. *If $p \in \mathbb{N}$ is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a$ mod p and, if p is not divided by a, then $a^{p-1} \equiv 1$ mod p.*

$$a^p = ((a-1)+1)^p \equiv (a-1)^p + 1^p \equiv (a-1)+1 = a \text{ mod } p$$

Since $a^{p-2}a = a^{p-1} \equiv 1$ mod p, we have

$$a^{-1} \equiv a^{p-2} \text{ mod } p.$$

4.4 Linear Diophantine equations

Let $a, f, g \in \mathbb{Z}$ be given, and suppose that we are looking for all integral solutions $s, t \in \mathbb{Z}$ of the linear Diophantine equations

$$sf + tg = a \tag{1}$$

The set of all real solutions of (1) is a line in the plane $\mathbb{R}^2$,that can be written as a sum $v + U$ of a particular solution $v \in \mathbb{R}^2$ and the set U of all solutions of the homogenous equation

$$sf + tg = 0 \tag{2}$$

Theorem 3. *Let* R *be a Euclidean domain,* $a, f, g \in R$*, and* $h = \gcd(f, g)$.

- *(1) has a solution* $(s, t) \in R^2$ *if and only if* h *divides* a.

- *If* $h \neq 0$ *and* $(s^*, t^*) \in R^2$ *is a solution of (1), then the set of all solutions is* $(s^*, t^*) + U$*, where*

$$U = R \cdot \left(\frac{g}{h}, -\frac{f}{h} \right) \subset R^2$$

is the set of all solutions to the homogenous equation (2).

- *If* $R = F[x]$ *for a field* $F, h \neq 0$, *(1) is solvable, and* $\deg f + \deg g - \deg h > \deg a$, *then there is a unique solution* $(s, t) \in R^2$ *of (1) such that* $\deg s < \deg g - \deg h$ *and* $\deg t < \deg f - \deg h$.

4.5 Continued fractions

The continued fraction expansion of $r_0/r_1 \in K$ where K is the field of fractions of R:

$$\frac{r_0}{r_1} = \frac{q_1 r_1 + r_2}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}}$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{q3 + \frac{r_4}{r_3}}} = \cdots = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_t}}}}$$

To abbreviate, we write $[q_1, \ldots, q_l]$ for the continued fraction $q_1 + 1/(q_2 + 1/(\cdots + 1/q_l)\cdots)$.

For example

$$\frac{126}{35} = \frac{18}{5} = [3, 1, 1, 2] = 3 + \frac{1}{1 + \frac{1}{1+\frac{1}{2}}}$$

An element $\alpha \in \mathbb{R}$ can be represented by (infinite) continued fraction in the sense that its initial segments converge to α w.r.t the absolute value.

It can be computed as follows: set

$$\alpha_1 = \alpha, q_1 = \lfloor \alpha_1 \rfloor, \beta_2 = \alpha_1 - q_1, \alpha_2 = 1/\beta_2, ...,$$
$$q_i = \lfloor \alpha_i \rfloor, \beta_{i+1} = \alpha_i - q_i, \alpha_{i+1} = 1/\beta_{i+1}$$

The expansion stops when $\beta_i = 0$, which occurs if and only if α_1 is rational.

The continued fraction expansion of an irrational number $\alpha \in \mathbb{R}$ is an excellent tool for approximate α by rational numbers with "small" denominator.

$$\left| a - \frac{p}{q} \right| \leq \frac{1}{cq^2}$$

For example, when $\alpha_1 = \sqrt{3}$, we obtain

$$\sqrt{3} = [1, 1, 2, \overline{1, 2} \ldots]$$

where the overlined part indicates the period of this ultimately periodic sequence. Euler(1737) showed that the continued fraction expansion is periodic for a root of an irreducible quadratic polynomial with integer coefficients; Lagrange(1770a) proved the converse.

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 1, 3, 1 \ldots]$$

" A large-scale calculation of π is entirely unforgiving; it soaks into all parts of the machine and a single bit awry leaves detectable consequences."